1 Základné pojmy

Väčšinu objektov, s ktorými sa budeme v matematike a informatike stretávať možno chápať ako *množiny* prvkov istých vlastností. Pod množinou si predstavujeme súbor objektov, ktoré majú nejakú spoločnú vlastnosť (napr. množina všetkých znakov slovenskej abecedy, množina prirodzených čísel – označujeme $\mathbb{N}$, ...). Objekty, ktoré tvoria množinu nazývame *prvkami* danej množiny. Viac o množinách si povieme v ďalšej kapitole, zatiaľ nám postačí takáto intuitívna predstava.

Matematika často náraba s nekonečným, resp. veľmi veľkým počtom objektov, ktoré sú idealizované a abstraktné (napríklad množina všetkých prirodzených čísel). Preto v matematike na rozdiel od iných vied nemáme možnosť overovať pravdivosť matematických tvrdení experimentálne na základe empirických poznatkov.

Ak chce matematik zaručiť platnosť nejakého matematického tvrdenia, musí ho *dokázať*, t.j. zostrojiť matematický dôkaz tohto tvrdenia. Napríklad v prípade, keď chce matematik dokázať existenciu objektu s nejakými vlastnosťami z malej množiny, t.j. z nie veľmi veľkého počtu objektov (napríklad množiny prirodzených čísel menších ako 100), môže postupne prebrať všetky prvky danej množiny a overiť, či niektorý z nich nemá požadované vlastnosti. Táto metóda je však nepoužiteľná pre množiny s nekonečným počtom objektov, ale i pre množiny s veľkým počtom objektov.

Matematický dôkaz je *deduktívny*, t.j. vychádza z pravdivých tvrdení (alebo z tvrdení, ktoré sa považujú za pravdivé) a vedie s použitím výlučne logických pravidiel k tvrdeniu, ktoré je nutne a za každých okolností pravdivé. Matematické dôkazy nie sú založené na názoroch, ktoré sa môžu meniť, alebo na skúsenostiach (experimentoch), ktoré možno zlepšovať alebo vyvracať. Keď je matematické tvrdenie raz korektne dokázané, nie je možné ho viac vyvrátiť a jediné, čo ho môže postihnúť je, že sa stane zvláštnym prípadom všeobecného tvrdenia.

Ak chceme porozumieť matematike, musíme sa naučiť rozumieť dôkazom matematických tvrdení. Preto sa v úvode zoznámime s výstavbou matematických teórií, jazyku matematiky a metódam matematických dôkazov.

1.1 Výstavba matematickej teórie

Čo je to matematická teória? Pozrime sa napríklad na teóriu množín, s ktorej základmi ste sa už zoznámili. Zisťujeme, že v každej matematickej teórii možno vyčleniť dve časti:

1. logické základy teórie,
2. vlastnú matematickú teóriu.

Logické základy teórie predstavuje logika (logický aparát), ktorý daná matematická teória používa. Logické základy matematickej teórie nemusia byť uvedené explicitne, matematici vedia, aký logický aparát treba použiť. Aby sme si utvorili určitú predstavu ako vyzerajú základy matematických teórií, predpokladajme, že používame výrokovú logiku. Výrokovú logiku zadávame súborom základných logických právd (logických axióm) a odvodzovacích pravidiel. Odvodzovacie pravidlá sú predpisy umožňujúce odvodiť z pravdivých tvrdení ďalšie pravdivé tvrdenia. Neskôr uvidíme, že všetky pravdivé tvrdenia výrokovej logiky možno odvodiť z relatívne malého počtu axióm pomocou jediného odvodzovacieho pravidla.

Samotné logické základy hovoria o tom, ako možno od pravdivých tvrdení prejsť opäť k pravdivým tvrdeniam, ale žiadne nové poznatky napr. o množinách z nich odvodiť nemožno. Aby sme vybudovali napríklad teóriu množín, musíme zaviesť pojmy množina, podmnožina, byť prvkom množiny, zjednotenie, ... Pojmy matematickej teórie sa delia na dve skupiny:

- základné pojmy – tieto v teórii zavádzame bez toho, aby sme ich popisovali (napr. množina, byť prvkom množiny);
- odvodené pojmy – tieto možno definovať pomocou základných pojmov (napr. podmnožina, zjednotenie).

Každú matematickú teóriu možo pokladať za sústavu výrokov o nejakých matematických objektoch. Je zrejmé, že pri deduktívnje metóde, ktorú matematika uplatňuje pri získavaní nových poznatkov, nie je možné každý poznatok (tvrdenie) odvodiť z iného (povedzme jednoduchšieho) poznatku. Ukazuje sa, že treba vychádzať z istých tvrdení, ktoré prehlásime za pravdivé a priori (tzv. axiómy), a z nich odvodzovať ďalšie poznatky prípustnými logickými prostriedkami. Takýmto spôsobom možno vybudovať celú teóriu. Axiómy formulujú v konečnom dôsledku isté vlastnosti základných pojmov, ktoré nedefinujeme, pokladáme za hotové, dané (napr. v axiomatickej geometrii sú takými pojmami bod a priamka).

Vlastné axiómy danej matematickej teórie možno spravidla vybrať viacerými spôsobmi. Existujú však (našťastie) aj kritériá, ktoré umožňujú posúdiť, či bol výber „dobrý“, alebo nie.

V modernej axiomatickej teórii nechápeme axiómy ako akési „samozrejmosti“, ale pokladáme ich za východiská celej teórie.

Okrem vlastných axióm existujú v matematickej teórii aj tzv. logické axiómy, ktoré sú spoločné pre viacero matematických teórií používajúcich tie isté logické základy.

Z vlastných i logických axióm možno potom pomocou odvodzovacích pravidiel odvodzovať tvrdenia, ktorých pravdivosť je rovnaká ako pravdivosť východiskových axióm. Tieto tvrdenia sa nazývajú teorémami danej matematickej teórie.

Vybudovať nejakú axiomatickú teóriu nie je spravidla jednoduchá úloha. Naším cieľom bude len naučiť sa pracovať s tvrdeniami matematických teórií, t.j. naučiť sa rozpoznávať logickú štruktúru matematických tvrdení a základné typy dôkazov matematických tvrdení.

1.2 Výroky

Výrok je tvrdenie, o ktorého pravdivosti alebo nepravdivosti má zmysel uvažovať. Výrok je buď pravdivý alebo nepravdivý (princíp dvojhodnotovosti); t.j. nemôže byť súčasne pravdivý i nepravdivý (zákon o vylúčení sporu), ale platí aspoň jedna z týchto možností (zákon vylúčenia tretieho).

Pravdivostná hodnota „pravdivý“ sa označuje symbolom 1 alebo T (true); pravdivostná hodnota „nepravdivý“ sa označuje symbolmi 0 alebo F (false). Pri rozhodovaní, či nejaké tvrdenie je výrokom, t.j. či má pravdivostnú hodnotu 0 alebo 1 z hľadiska výrokového počtu nazáleží na tom, akým spôsobom zistíme pravdivostnú hodnotu daného tvrdenia, dokonca ani na tom, či vôbec vieme pravdivostnú hodnotu tvrdenia určiť.

Príklad 1.1.

A. Uveďme nejaké príklady výrokov s udaním ich pravdivostnej hodnoty:

(T): Číslo -3 je menšie ako 0. (F): Mačka nie je cicavec. (T): Každý človek je smrteľný.

(T): Pre ľubovoľné prirodzené číslo n, $n \geq 3$ nasledujúca rovnica nemá riešenie v prirodzených číslach x, y, z:

$$x^n + y^n = z^n.$$

Slávna Fermatova veta dokázaná iba nedávno.

B. Nasledujúce tvrdenia sú tiež výrokmi, aj keď ich pravdivostná hodnota nie je zatiaľ známa.

(?): Každé párne číslo väčšie ako 2 možno rozložiť na súčet dvoch prvočísel (Goldbachova domnienka).

A	non A
0	1
1	0

Tabuľka 1: Pravdivostné hodnoty negácie

(?): Na Marse existuje živá hmota.

C. Výrokmi nie sú nezmyslené tvrdenia, ale napr. i opytovacie vety, rozkazovacie vety. Nasledujúce tvrdenia nie sú výrokmi:

Táto veta je zelená. Súčasný kráľ USA je černoch. Koľko je hodín? Zavrite dvere!

D. Výrokmi nie sú ani nasledujúce tvrdenia, pretože im nemožno priradiť pravdivostnú hodnotu:

Táto veta je nepravdivá. Všetci Kréťania vždy klamú (hovorí Kréťan).

Výroky označujeme veľkými písmenami latinskej abecedy: $A, B, C, \ldots$, nazývame ich tiež výrokovými premennými. Pravdivostnú hodnotu výroku A budeme označovať symbolom $h(A)$.

Ak sú A, B ľubovoľné výroky, tak z nich pomocou logických spojok možno vytvárať nové výroky. Najjednoduchší spôsob ako zmeniť výrok je zrejme popretie skutočnosti, ktorú vyjadruje, t.j. súhlas s protikladnou skutočnosťou. Výrok B, ktorý je protikladom výroku A nazveme *negáciou výroku* A a budeme ho označovať $\neg A$ (niekedy sa používa aj označenie A', $\overline{A}$, non A, alebo v programovacích jazykoch NOT A). Pravdivostnú hodnotu výroku $\neg A$ popisuje pravdivostnostná tabuľka číslo 1:

Konjunkcia spája výroky A, B do nového výroku „A a B“. Konjunkciu označujeme výrazom $A \wedge B$ (alebo AB, resp. A AND B). Konjunkcia $A \wedge B$ je pravdivá práve vtedy, ak sú pravdivé výroky A, B.

Disjunkciu výrokov A, B znamená výrok, ktorý čítame „A alebo B“. Disjunkciu výrokov A, B zapisujeme výrazom $A \vee B$ (alebo A OR B). Disjunkcia $A \vee B$ je pravdivá práve vtedy, ak je pravdivý aspoň jeden z výrokov A alebo B. Okrem disjunkcie sa niekedy používa tzv. *alternatíva* (sčítanie podľa modulo 2 alebo XOR spájanie), ktorú čítame „buď platí A alebo platí B, ale A a B neplatí súčasne“. Alternatívu výrokov A, B zapisujeme výrazom $A \oplus B$ a je pravdivý práve vtedy, ak je pravdivý práve jeden z výrokov A, B.

V matematických dôkazoch zohráva veľmi dôležitú úlohu *implikácia*. Implikácia výrokov A, B sa označuje symbolicky ako $A \Rightarrow B$ a číta sa „ak A, tak B“, „A implikuje B“, „z A vyplýva B“. Výrok A sa v implikácii nazýva *predpoklad – premisa* a výrok B *uzáver – conclusio*, ktorý sa v matematike nazýva aj tvrdením. Implikácia je nepravdivá v prípade, keď predpoklad je pravdivý a dôsledok nepravdivý. V ostatných prípadoch je implikácia pravdivá.

Ekvivalenciu výrokov A, B zapisujeme výrazom $A \sim B$ (alebo $A \equiv B$) a čítame ako „A je ekvivalentné s B“, A práve vtedy keď B“, „A vtedy a len vtedy, keď B“. Ekvivalencia $A \equiv B$ platí vtedy, ak majú výroky A, B rovnakú pravdivostnú hodnotu. V takomto prípade sa výroky nazývajú *logicky rovnocenné (ekvivalentné)*. To, že výroky majú rovnakú pravdivostnú hodnotu znamená, že jeden z nich môže byť napríklad v zloženom výroku nahradený druhým bez toho, aby sa zmenila pravdivostná hodnota zloženého výroku. Na druhej strane však logicky ekvivalentné výroky nemusia mať rovnaký zmysel. (Napríklad výroky „11.9.2000 bol pondelok“ a „$\pi > 3$“ sú pravdivé a teda ekvivalentné výroky, ktoré však majú rozličný zmysel.)

Nahrádzanie výrokov ekvivalentnými výrokmi využívame pri zjednodušovaní zložených výrokov.

Ak je pravdivostná hodnota výroku identicky rovná 1, t.j. výrok je pravdivý pre všetky možné kombinácie pravdivostných hodnôt výrokov, ktoré obsahuje, nazývame ho *tautológia*. Výrok, ktorého pravdivostná hodnota sa identicky rovná 0 sa nazýva *kontradikciou*.

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \oplus B$	$A \equiv B$
0	0	0	0	1	0	1
0	1	0	1	1	1	0
1	0	0	1	0	1	0
1	1	1	1	1	0	1

Tabuľka 2: Pravdivostné hodnoty zložených výrokov

Uveďme niektoré významné logické tautológie, ktoré budeme v ďalšom využívať.

Veta 1.2. Nech A, B, C sú ľubovoľné výroky (výrokové premenné), symbol 0 (resp. 1) označuje ľubovoľné kontradikcie (resp. tautológie). Potom sú nasledujúce výroky tautológie:

i. $(A \vee A) \equiv A$, $(A \wedge A) \equiv A$ (idempotentnosť),

ii. $(A \wedge B) \equiv (B \wedge A)$, $(A \vee B) \equiv (B \vee A)$, $(A \equiv B) \equiv (B \equiv A)$ (komutatívnosť)

iii. $(A \vee (B \vee C)) \equiv ((A \vee B) \vee C)$, $(A \wedge (B \wedge C)) \equiv ((A \wedge B) \wedge C)$ (asociatívnosť)

iv. $(A \vee (B \wedge C)) \equiv (A \vee B) \wedge (A \vee C)$, $(A \wedge (B \vee C)) \equiv (A \wedge B) \vee (A \wedge C)$ (distributívne zákony)

v. $(A \wedge (B \vee A)) \equiv A$, $(A \vee (B \wedge A)) \equiv A$ (absorpčné zákony)

vi. $(\neg\neg A) \equiv A$ (zákon dvojitej negácie)

vii. $A \vee (\neg A)$ (zákon vylúčenia tretieho)

viii. $(\neg(A \wedge B)) \equiv ((\neg A) \vee (\neg B))$, $(\neg(A \vee B)) \equiv ((\neg A) \wedge (\neg B))$ (de Morganove zákony)

ix. $(\neg A \Rightarrow \neg B) \equiv (B \Rightarrow A)$ (kontrapozícia negácie)

x. $(A \equiv B) \equiv ((A \Rightarrow B) \wedge (B \Rightarrow A))$

xi. $(A \wedge B) \equiv (\neg((\neg A) \vee (\neg B))$

xii. $(A \vee B) \equiv (\neg((\neg A) \wedge (\neg B))$

xiii. $(A \Rightarrow B) \equiv (\neg A \vee B))$

xiv. $A \Rightarrow (B \Rightarrow A)$

xv. $((\neg A) \Rightarrow A) \Rightarrow A$ (reductio ad absurdum)

xvi. $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

xvii. $(\neg A \Rightarrow \neg B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow A)$

xviii. $(A \wedge B) \Rightarrow A$, $(A \wedge B) \Rightarrow B$

xix. $A \Rightarrow (A \vee B)$, $B \Rightarrow (A \vee B)$

xx. $(A \wedge \neg A) \equiv 0$, $(A \vee \neg A) \equiv 1$

xxi. $(A \wedge 1) \equiv A$, $(A \wedge 0) \equiv 0$

xxii. $(A \vee 0) \equiv A$

xxiii. $(A \Rightarrow 0) \equiv \neg A$, $(A \Rightarrow 1) \equiv 1$

xxiv. $(1 \Rightarrow A) \equiv A$

1.3 Výrokové formy

Niekedy sa v matematike stretávame s formálnymi výrazmi (formulami), ktoré obsahujú nejaký symbol (napr. x) a majú tú vlastnosť, že ak za x dosadíme vhodný objekt, dostaneme výrok. Takéto formuly nazývame *výrokovými funkciami* alebo *výrokovými formami*.

Príklad 1.3. Nasledujúce tvrdenia sú výrokovými formami: x je prvočíslo, x je väčšie ako 3, x nemá výťah.

Ku každej výrokovej forme existuje nejaká množina $\mathcal{M}$ objektov, ktoré má zmysel do výrokovej formy dosadzovať. Označme $A(x)$ výrokovú formu definovanú na množine prirodzených čísel napríklad takto:

$$A(x) : x \text{ je väčšie ako } 3.$$

Dosadzovaním prirodzených čísel do formuly $A(x)$ dostávame výroky, t.j. tvrdenia s pravdivostnou hodnotou:

$$\begin{array}{lcll} a(1) & : & 1 > 3 & F \\ a(2) & : & 2 > 3 & F \\ a(3) & : & 3 > 3 & F \\ a(4) & : & 4 > 3 & T \\ \ldots & & & \end{array}$$

Z výrokovej formy môžeme dostať výrok nielen dosadením vhodného objektu, ale aj tým, že určíme (kvantifikujeme), pre koľko (aké množstvo) prvkov z množiny $\mathcal{M}$ dáva daná výroková forma výrok.

Kvantifikované výroky vytvárame pomocou dvoch typov kvantifikátorov:

- „pre všetky“ – označujeme $\forall$ – všeobecný (veľký) kvantifikátor,
- „existuje“ – označujeme $\exists$ – existenčný (malý) kvantifikátor.

Príklad 1.4. Nech $A(x)$ označuje výrokovú formu „x je väčšie ako 3“ definovanú na množine prirodzených čísel. Potom tvrdenie „existuje x tak, že platí $A(x)$“ označuje (pravdivý) výrok, ktorý zapíšeme nasledovne:

$$\exists x\,((x \in \mathbb{N}) \wedge (x > 3)).$$

Tvrdenie „pre všetky x platí $A(x)$“ označuje (nepravdivý) výrok, ktorý zapíšeme nasledovne:

$$\forall x\,((x \in \mathbb{N}) \Rightarrow (x > 3)).$$

Ak je zrejmé, pre ktoré hodnoty je definovaná výroková forma $A(x)$, používame aj skrátený zápis:

$$\forall x\, A(x) \quad \text{alebo} \quad \exists x\, A(x).$$

Poznámka. Predpokladajme, že výroková forma $A(x)$ je definovaná na konečnej množine $N_n = \{0, 1, \ldots, n\}$ Potom kvantifikované výroky $\forall x\, A(x)$ a $\exists x\, A(x)$ možno vyjadriť aj takto:

$$\begin{aligned} \forall x\, A(x) &\equiv a(0) \wedge a(1) \wedge \ldots \wedge a(n) \wedge 1, \\ \exists x\, A(x) &\equiv a(0) \vee a(1) \vee \ldots \vee a(n) \vee 0. \end{aligned}$$

Pomocou takéhoto zápisu môžeme ľahko určiť pravdivostné hodnoty formúl $\forall x\, A(x)$ a $\exists x\, A(x)$ aj v prípade, keď je množina hodnôt premennej x prázdna.

Kvantifikované výroky môžme spájať pomocou logických spojok. Zvláštnu pozornosť si zasluhuje negovanie kvantifikovaných výrokov.

$$\begin{aligned} \neg(\forall x\, A(x)) &\equiv \exists x\, (\neg A(x)) \\ \neg(\exists x\, A(x)) &\equiv \forall x\, (\neg A(x)). \end{aligned}$$

Príklad 1.5. Nech $A(x)$ označuje výrokovú formu „x je prvočíslo“ definovanú na prirodzených číslach.

1. Uvažujme kvantifikovaný výrok $\exists x\, A(x)$, t.j.

$$\exists x\, A(x) : \quad \exists x\, [(x \in \mathbb{N}) \wedge x \text{ je prvočíslo})].$$

Postupnou negáciou dostávame:

$$\neg\exists x\, [(x \in \mathbb{N}) \wedge (x \text{ je prvočíslo})] \equiv \forall x\, \neg[(x \in \mathbb{N}) \wedge (x \text{ je prvočíslo})]$$

čo uplatnením de Morganovho zákona môžeme upraviť na tvar

$$\forall x\, \neg[(x \in \mathbb{N}) \wedge (x \text{ je prvočíslo})] \equiv \forall x\, [\neg(x \in \mathbb{N}) \vee \neg(x \text{ je prvočíslo})].$$

Vzhľadom k definičnému oboru je posledná disjunkcia ekvivalentná s výrokovou formou $\forall x[\neg(x$ je prvočís

2. Uvažujme kvantifikovaný výrok

$$\forall x\, A(x) : \quad \forall x\, [(x \in \mathbb{N}) \Rightarrow (x \text{ je prvočíslo})].$$

Negujeme tento výrok a postupnými úpravami dostávame:

$$\neg\forall x\, [(x \in \mathbb{N}) \Rightarrow (x \text{ je prvočíslo})] \equiv \exists x\, [(x \in \mathbb{N}) \wedge \neg(x \text{ je prvočíslo})].$$

Doteraz sme používali výrokové formy s jednou premennou, podobným spôsobom môžme zaviesť výrokové formy viacerých premenných, napr. $b(x, y)$ bude označovať výrokovú formu dvoch premenných x, y: $x > y$. Pomocou kvantifikátorov možno z danej výrokovej formy vytvoriť 8 výrokov.

1.4 Matematické dôkazy

Z doterajšieho štúdia matematiky máme aspoň intuitívnu predstavu o tom, ako vyzerá matematický dôkaz. Ak nie, tak pre naše potreby úplne postačí, ak si pod matematickým dôkazom tvrdenia B budme predstavovať postupnosť tvrdení $A_1, \ldots, A_n = B$, kde A_i sú nejaké výroky alebo výrokové formy a pre všetky i, $i = 1, \ldots, n-1$ sú implikácie $A_i \Rightarrow A_{i+1}$ tautológie.

Jedným z našich cieľov bude upresniť túto predstavu a naučiť sa štandardným postupom, ktoré sa pri dôkazoch matematických tvrdení používajú.

Základné typy matematických dôkazov:

1. priame dôkazy,

2. nepriame dôkazy,

3. dôkazy matematickou indukciou.

Vo všetkých typoch deduktívnych dôkazov potrebujeme mať k dispozícii odvodzovacie pravidlá, ktoré nám umožnia prejsť od pravdivých tvrdení k novým pravdivým tvrdeniam. Najdôležitejším odvodzovacím pravidlom, ktoré budeme používať, je tzv. pravidlo odlúčenia, *modus ponens*, ktoré zapisujeme v nasledujúcom tvare:

$$\frac{A \Rightarrow B, A}{B}.$$

Zmysel tohoto pravidla je nasledujúci – ak platia výroky napísané nad čiarou (predpoklady), tak potom musí platiť aj záver, t.j. výrok B.

Pravidlo modus ponens možno napísať aj v nasledujúcom tvare:

$$\frac{\neg B \Rightarrow \neg A, \neg B}{\neg A}.$$

Ak ma implikáciu v predpoklade použijeme pravidlo kontrapozície negácie dostávame pravidlo nazývané *modus tolens*:

$$\frac{A \Rightarrow B, \neg B}{\neg A}.$$

Ďalšie dôležité pravidlo je *pravidlo sylogizmu*, ktoré umožňuje skracovať dlhé reťazce implikácií v dôkaze:

$$\frac{A \Rightarrow B, B \Rightarrow C}{A \Rightarrow C}.$$

1.4.1 Priamy dôkaz

Priamy dôkaz matematického výroku, tzv. tvrdenia spočíva v tom, že z už dokázaných výrokov (viet) získame tvrdenie po konečnom počte korektných úsudkov.

Schématicky (zjednodušene) vyzerá priamy dôkaz asi takto: je daný predpoklad A, potrebujeme dokázať dôsledok B. Postupne odvodzujeme tvrdenia $A \Rightarrow A_1$, $A_1 \Rightarrow A_2$, $A_2 \Rightarrow A_3$, ..., $A_{n-1} \Rightarrow A_n$, $A_n \Rightarrow B$, kde $A_1, \ldots, A_n$ sú nejaké výroky. Použitím pravidla sylogizmu dostávame:

$$\frac{A \Rightarrow A_1, A_1 \Rightarrow A_2}{A \Rightarrow A_2}, \frac{A_2 \Rightarrow A_3, A_3 \Rightarrow A_4}{A_2 \Rightarrow A_4}, \ldots$$

Tento postup budeme opakovať dovtedy, kým nám nezostane jediná implikácia $A \Rightarrow B$. Keďže sme predpokladali platnosť A, môžeme použiť pravidlo modus ponens a dostávame potrebný záver, t.j. platnosť B.

Príklad 1.6. Dokážeme priamo nasledujúce tvrdenie o prirodzených číslach: ak x je párne prvočíslo, potom nie je deliteľné 3.

Ak x je párne prvočíslo, potom nutne $x = 2$. Číslo 2 nie je deliteľné 3. Použitím sylogizmu na predchádzajúce 2 výroky dostávame požadované tvrdenie.

1.4.2 Nepriamy dôkaz

Predpokladáme, že je pravdivý predpoklad A. Potrebujeme odvodiť B. Ak by sa nám podarilo odvodiť $A \Rightarrow B$, tak môžeme použiť pravidlo modus ponens a odvodíme platnosť B. S odvodením implikácie $A \Rightarrow B$ však môžu byť ťažkosti.

Pravdivosť implikácie $A \Rightarrow B$ môžeme nepriamo dokázať tak, že dokazuje platnosť jej kontrapozície $\neg B \Rightarrow \neg A$, alebo predpokladáme platnosť opačného tvrdenia $\neg(A \Rightarrow B)$, t.j. $(A \wedge \neg B)$ a snažíme sa odvodiť *spor*.

V prípade sporu môže nastať jeden z týchto troch prípadov:

1. dostaneme spor s predpokladom A: t.j. dokážeme platnosť implikácie $\neg(A \Rightarrow B) \Rightarrow \neg A$, t.j. platnosť $A \Rightarrow (A \Rightarrow B)$ a z platnosti A vyplýva platnosť $A \Rightarrow B$.

2. dostaneme spor s predpokladom $\neg B$: t.j. dokážeme platnosť implikácie $\neg(A \Rightarrow B) \Rightarrow B$. Použitím tautológie $B \Rightarrow (A \Rightarrow B)$ a pravidla sylogizmu dostávame: $\neg(A \Rightarrow B) \Rightarrow (A \Rightarrow B)$ a z predpokladov platnosti $\neg(A \Rightarrow B)$ dostávame platnosť $(A \Rightarrow B)$.

3. dostaneme dva navzájom si odporujúce výroky S a $\neg S$: t.j. dokážeme platnosť implikácie $\neg(A \Rightarrow B) \Rightarrow (S \wedge \neg S)$. Použitím kontrapozície negácie a de Morganových zákonov $(\neg(S \wedge \neg S) \equiv (\neg S \vee S))$ dostávame:
$$(\neg S \vee S) \Rightarrow (A \Rightarrow B),$$
pričom ľavá strana je tautológia a teda dostávame platnosť $A \Rightarrow B$ použitím pravidla modus ponens.

Účinnosť nepriamych dôkazov závisí podstatne na tom, že okrem daných predpokladov sa naviac ako predpoklad prijme nepravdivosť toho, čo sa tvrdí a vychádza sa teda z väčšieho počtu predpokladov. Vďaka tomu sa mnohé tvrdenia dokazujú ľahšie nepriamo, ako keby sa mali dokazovať priamo.

Príklad 1.7. Dokážeme tvrdenie z predchádzajúceho príkladu nepriamo (sporom): Predpokladáme, že platí: „x je párne prvočíslo a zároveň x je deliteľné tromi.“ To ale znamená, že x má deliteľov 1, 2, 3 (a x), a teda nie je prvočíslom (spor).

1.4.3 Rozlišovacia metóda

Ak je množina hodnôt, ktoré možno dosadzovať do výrokových funkcií konečná, potom možno overiť pravdivosť kvantifikovaných výrokov dosadením konečného počtu prvkov. Takéto dôkazy sa nazývajú *verifikácie*. Keď sa všetky možnosti rozdelia do rozličných skupín a dôkaz sa spraví pre každú skupinu, hovoríme o rozlišovaní prípadov alebo o rozlišovacej metóde. Podstatné je, aby sa pri rozdelení nezabudlo na žiaden prípad.

Táto metóda však už aj pri niektorých pomerne jednoduchých úlohách vedie k ťažkostiam, spojených s veľmi veľkým počtom prvkov, ktoré treba uvažovať. Ako príklad uveďme šachy, či je číslo $2^{(2^{13})} + 1$ prvočíslo, ...

Výrok kvantifikovaný všeobecným kvantifikátorom možno vyvrátiť jediným prípadom, tzv. *kontrapríkladom*.

Tvrdenie $\forall x\ (x \in M \Rightarrow x$ má vlastnosť $A)$ vyvrátime, ak nájdeme prvok x_0, ktorý patrí do M, ale vlastnosť A nemá.

Metóda kontrapríkladu patrí k základným prostriedkom práce matematika: matematik najskôr preskúma neznáme skutočnosti pomocou príkladov a kontrapríkladov a až potom začne získané skutočnosti zovšeobecňovať tak, aby neboli logicky napadnuteľné.

Príklad 1.8. (a) Každé nepárne číslo je prvočíslo. Tvrdenie neplatí, kontrapríkladom je 9.
(b) Každé prvočíslo je nepárne číslo. Tvrdenie neplatí, kontrapríkladom je 2.

1.4.4 Matematická indukcia

V niektorých (väčšine) matematických disciplín sa veci počítajú a vyslovujú sa výroky na prirodzených číslach. Mimoriadnu dôležitosť má preto metóda, nazývaná *metódou úplnej* alebo *matematickej indukcie*, ktorá umožňuje ukázať pravdivosť výrokovej formy kvantifikovanej všeobecným kvantifikátorom, ktorej premenné nadobúdajú hodnoty z množiny prirodzených čísel.

Princíp matematickej indukcie Nech je daná výroková formula $A(n)$ definovaná pre všetky prirodzené čísla n a nech platí:

1. $A(1)$ je pravdivý výrok (báza indukcie)
2. pre každé n z platnosti výroku $A(n)$ vyplýva platnosť výroku $A(n+1)$ (indukčný krok)

Potom platí $A(n)$ pre všetky prirodzené čísla.
Princíp matematickej indukcie je jednou z axióm matematickej teórie, nazývanej *formálnou aritmetikou.*

Poznámka. Iný variant metódy úplnej indukcie môžeme dostať nasledovnou modifikáciou kroku 2 v predchádzajom princípe: pre každé n z platnosti výrokov $A(1), \ldots, A(n)$ vyplýva platnosť výroku $A(n+1)$ (indukčný krok).

Poznámka. V niektorých prípadoch je výhodné používať modifikovaný princíp matematickej indukcie, v ktorom sa v prvom kroku (t.j. v báze indukcie) predpokladá platnosť formuly $A(i)$ pre nejakú hodnotu $i = n_0$. Je zrejmé, že princíp matematickej indukcie v pôvodnej podobe je špeciálnym prípadom modifikovaného princípu matematickej indukcie (pre $n_0 = 1$).

Príklad 1.9. Matematickou indukciou dokážeme, že pre súčet geometrickej rady 2^i platí nasledujúci vzorec: $\sum_{i=0}^{n} 2^i = 2^n$.
1. Vzťah $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ je správny pre $n = 1$, ako sa presvedčíme dosadením.
2. Predpokladajme, že uvedený vzťah platí pre nejakú hodnotu $n = n_0$. Dokážeme, že platí aj pre $n = n_0 + 1$. Skutočne,

$$\sum_{i=0}^{n_0+1} 2^i = \left(\sum_{i=0}^{n_0} 2^i\right) + 2^{n_0+1};$$

suma v zátvorke je podľa predpokladu rovná $2^{n_0+1} - 1$, takže

$$\sum_{i=0}^{n_0+1} 2^i = 2^{n_0+1} - 1 + 2^{n_0+1} = 2 \cdot 2^{n_0+1} - 1 = 2^{n_0+2} - 1,$$

čo je požadovaný vzťah pre $n = n_0 + 1$.

Nasledujúci príklad ukazuje, že pri dôkaze matematickou indukciu nemožno vynechať žiaden z predpokladov:

Príklad 1.10. Dokážeme, že súčet geometrického radu $1 + q + q^2 + \ldots + q^n$ sa pre $q \neq 1$ rovná:

$$\frac{q^{n+1} - q}{q - 1}.$$

Vynecháme dôkaz bázy indukcie a prejdeme hneď k dôkazu indukčného kroku. Ak pre ľubovoľné prirodzené číslo n platí

$$1 + q + \ldots + q^n = \frac{q^{n+1} - q}{q - 1}, \qquad (q \neq 1),$$

potom

$$1 + q + \ldots + q^n + q^{n+1} = \frac{q^{n+1} - q}{q - 1} + q^{n+1} = \frac{q^{n+1} - q}{q - 1} + \frac{q^{n+2} - q^{n+1}}{q - 1} = \frac{q^{n+2} - q}{q - 1};$$

t.j. ak súčtový vzorec platí pre n, platí aj pre $n + 1$.
Napriek tomu uvedený rad nemá taký súčet, pretože neplatí báza indukcie (overiť)!

Matematickú indukciu nemožno používať bezmyšlienkovite, mechanicky. Nasledujúci príklad ukazuje, aké problémy môžu nastať, keď nevhodne zvolíme hodnotu pre bázu indukcie:

Príklad 1.11. Nedôslednou matematickou indukciu dokážeme, že každých n prirodzených čísel je zhodných. V prípade $n = 1$ nie je čo dokazovať (začiatok indukcie). Predpokladajme, že každých n čísel je rovnakých. Ukážeme, že potom aj každých $n + 1$ čísel je rovnakých. Vezmime čísla z_1, z_2, ..., z_{n+1}. Najprv vyškrtnime z_1, zostáva nám n čísiel a podľa indukčného predpokladu

$$z_2 = z_3 = z_4 = \ldots = z_n = z_{n+1}.$$

Podobne po vyškrtnutí z_{n+1} máme

$$z_1 = z_2 = z_3 = \ldots = z_n = z_n.$$

Z toho vyplýva

$$z_1 = z_2 = z_3 = z_4 = \ldots = z_n = z_{n+1}.$$

Kde je chyba? Chýba nám začiatok indukcie, prípad $n = 1$ je len zdanlivý začiatok. Princíp porovnávania možno použiť len pre $n \geq 2$ a začiatok indukcie je teda $n = 2$.